How To Create Keys On Command Line

NOTE: it should not be necessary to create SSL keys for Sentry SSO from the appliance command line. Please follow the instructions for creating keys using the CMI.

Contents

Creating DSA Private Key

DSA key generation involves two steps, and can be done through the command line on a Swivel virtual or hardware appliance:

```
openssl dsaparam -out dsaparam.pem 2048
openssl gendsa -out dsaprivkey.pem dsaparam.pem
```

The first step creates a DSA parameter file, dsaparam.pem, which in this case instructs OpenSSL to create a 2048-bit key in Step 2. The dsaparam.pem file is not itself a key, and can be discarded after the public and private keys are created. The second step actually creates the private key in the file dsaprivkey.pem which should be kept secret.

Creating RSA Private Key

RSA key generation involves a single command and can be done through the command line on a Swivel virtual or hardware appliance:

```
openssl genrsa -des3 -out rsaprivkey.pem 2048
```

This instructs OpenSSL to create a 2048-bit key in the file rsaprivkey.pem which should be kept secret.

Exporting Keys

Export the key into a DER (binary) format. You can do so with the following steps:

For DSA

```
openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
```

For RSA

```
openssl rsa -in rsaprivkey.pem -outform DER -pubout -out rsapubkey.der
openssl pkcs8 -topk8 -inform PEM -outform DER -in rsaprivkey.pem -out rsaprivkey.der -nocrypt
```

Step 1 extracts the public key into a DER format. Step 2 converts the private key into the pkcs8 and DER format. Once you've done this, you can use this public (dsapubkey.der/rsapubkey.der) and private (dsaprivkey.der/rsapubkey.der) key pair.

Creating a Certificate

Once you have your key pair, it's easy to create an X.509 certificate. The certificate holds the corresponding public key, along with some metadata relating to the organization that created the certificate. Follow this step to create a self-signed certificate from either an RSA or DSA private key:

```
openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
```

OR

```
openssl req -new -x509 -key rsaprivkey.pem -out rsacert.pem
```

After you answer a number of questions, the certificate will be created and saved as dsacert.pem or rsacert.pem